

10 January 1984

SUBJECT: Basic Requirement for Individual Access to CIA/DO  
Information Reports Contained in Computer Data  
Banks Such as DIA/SAFE and CIA/SAFE

Strict adherence to the need-to-know principle as defined in DCID 1/7 is a fundamental element in good security and an essential concept which must be applied without compromise. Need-to-know is defined in DCID 1/7 as "A determination by an authorized holder of classified information that access to specific classified material in his or her possession is required by one or more other persons to perform a specific and officially authorized function essential to accomplish a national security task.... In addition to an established 'need-to-know,' a person must possess an appropriate security clearance and access approvals, as required, prior to being provided classified information."

It is quite apparent to us that this directive draws a clear distinction between "access approval" and "need-to-know" since it deals with them as two separate stages or steps through which an individual may have to go to obtain access to classified information. The fact that an individual has been given an "access approval" for communications intelligence or overhead reconnaissance material should not entitle or permit access by that individual to all available information bearing those "access approval" code words. Need-to-know for specific subjects or categories of information must also be demonstrated or be apparent for the individual concerned.

We are very much aware that over the years there has been a gradual erosion in libraries, data banks, and other repositories of intelligence information of efforts to enforce strict need-to-know access. More and more, largely because it is easier to administer, access to information data banks has been granted on the basis of "access controls" and security clearances without regard to real need-to-know access controls. Some have attempted to offer the rationalization that if an individual is approved for the very sensitive "access control" code word information it must be acceptable that he have access to the entire range of topics contained in a data base. No matter how many access control approvals an individual may have, we would argue that there must be the further demonstrated need-to-know before specific topical access can be permitted.

C O N F I D E N T I A L

d. The extent to which compartmentation controls will be required, in CIRS security stage 1 or later, to limit automatic access on the basis of topical/geographic need-to-know (defined by original distribution to the office level and retained dissemination controls), as distinct from security clearances and code-word access approvals.